Math 314 - Fall 2016 **Name:**

Mission 8 Due December 11th, 2017

The driving force behind modern computer ciphers isnt security, but efficiency. The question is not can you create a secure cipher. You can. The question is whether you can create one that will work efficiently on huge data sets, or on very limited hardware.

— Jeff Dege.

Guidelines

- All work must be shown for full credit.
- You can choose to use SageMath code to help you solve the problems. If you do, print out your code (or use the same folder as the latex code on SMC).
- Either print out this assignment and write your answers on it, or edit the latex source on SMC and type your answers in the document. Make sure you still show your work! There is one point of extra credit available on this assignment if you use LaTeX
- You may work with classmates, but be sure to turn in your own written solutions. Write down the name(s) of anyone who helps you.
- Check one:
  ☐ I worked with the following classmate(s): _____
  ☐ I did not receive any help on this assignment.

1. Graded Problems

1. Using the primes $q = 113$, $p = 2 \times q + 1 = 227$, implement the discrete log hash. Use the sage command `primitive_root()` to find a primitive root, and find the digest of 35120.

2. Create an RSA key by using the primes $p = 1987$, $q = 2017$ and $e = 17$. Use the RSA signature algorithm to sign the message $m = 11235$. Then repeat this by signing the digest of the message when using the discrete log hash as described in problem 1.

3. My RSA key is $(n, e) = (5737043443, 3)$. You receive two messages from me, $(m_1, s_1) = (2357111317, 5014697870)$ and $(m_2, s_2) = (1357111317, 3012698810)$. Determine which one was forged without factoring n.

4. Describe how Eve could perform a Man-in-the-middle attack against the three-pass-protocol. (Page 83)

5. Let p be a large prime, and α a primitive root $\pmod{p}$. Let $h(x) \equiv \alpha^x \pmod{p}$. Why is $h(x)$ not a good cryptographic hash function?

6. (Note: For this problem do your work by hand, showing all of your work to receive full credit rather than using SAGE.) In the ElGamal Cryptosystem, Alice and Bob use $p = 17$ and $\alpha = 3$. Bob chooses his secret to be $a = 6$ so $\beta = 15$.
   a. Alice picks the secret number $k = 10$, and wishes to send the message $m = 2$ Determine the encrypted message that Alice sends to Bob.

b. Bob receives the ciphertext $(r, t) = (7, 6)$. Determine the plaintext m.